

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-195735

(43)Date of publication of application : 30.07.1996

(51)Int.Cl.

H04K 1/00

G09C 1/00

H04H 1/00

H04L 9/28

(21)Application number : 07-005792

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 18.01.1995

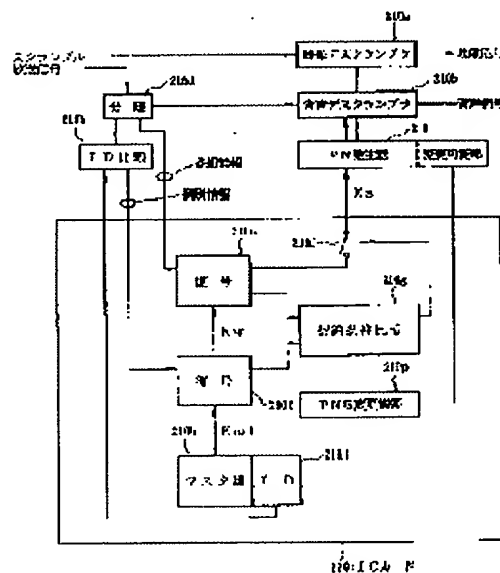
(72)Inventor : OI SHINICHI

(54) DECODER

(57)Abstract:

PURPOSE: To keep secrecy by transiting a state sequentially from a state given by a scramble key and generating a PN signal based on a conversion logic from the state to be transited thereby making the logic changeable.

CONSTITUTION: Since a PN generator 310 revises a logic to generate a PN signal, the initial state of the generator 310 is transited sequentially based on PN information 210p when the PNG information 210p is available. A PN signal is given to a video descrambler 210a and an audio descrambler 210b based on the transition, from which descrambled video signal and audio signal are obtained. When PNG information 210p of an IC card 220 is given newly to the generator 310, the state transition is made different based on the new information 210p, a different PN signal is generated and descrambling is conducted based on the new PN signal. Since the logic for generating the PN signal is variable, the security is improved.



(11)特許出願公開番号

(43)公開日 平成8年(1996)7月30日

技術表示箇所

A

審査請求 未請求 請求項の数11 OL (全 20 頁) 最終頁に続く

(74) 代理人 弁護士 三好 秀和 (外3名)

[illegible]

220: ICカード

【特許請求の範囲】

【請求項 1】 スクランブルされた信号を P N 信号を用いてデスクランブルするデコーダ装置であって、前記 P N 信号を用いて前記スクランブルされた信号をデスクランブルするデスクランブラと、スクランブルキーによって与えられた状態から順次状態遷移し、この遷移する状態から変換ロジックに基づいて前記 P N 信号を生成すると共に、前記 P N 信号生成のためのロジックが変更可能である P N 発生器と、前記スクランブルされた信号からスクランブルキーを復号すると共に、前記スクランブルキー及び前記 P N 信号生成ロジックを定めるための情報を前記 P N 発生器にあたる制御部と、を備えたデコーダ装置。

【請求項 2】 前記 P N 発生器は、前記遷移する状態から前記 P N 信号を得るための信号を変換ロジックに基づいて生成すると共に、前記変換ロジックが変更可能である非線形ロジックを含んで構成されていることを特徴とする請求項 1 記載のデコーダ装置。

【請求項 3】 前記 P N 発生器は、前記スクランブルキーによって与えられた初期状態から順次状態遷移するとともに、その状態出力が変更可能であるレジスタ回路部と、前記レジスタ回路部の状態出力を変換し前記 P N 信号を得るための信号を生成するロジック回路部と、を含んで構成されていることを特徴とする請求項 1 記載のデコーダ装置。

【請求項 4】 前記 P N 発生器は、前記スクランブルキーによって与えられた初期状態から順次状態遷移すると共に、その状態遷移のロジックが変更可能である線形フィードバックレジスタを含んで構成されていることを特徴とする請求項 1 記載のデコーダ装置。

【請求項 5】 前記制御部は、I D が書き込まれた I C カード上に構成され、前記スクランブルされた信号とともに送られた I D と前記 I C カード上の I D とが一致したときに前記スクランブルキーを前記 P N 発生器にあたることを特徴とする請求項 1 記載のデコーダ装置。

【請求項 6】 前記 I C カードの電源の状態を検出するための電源電圧検出回路をさらに有し、前記制御部は、前記 I C カードが本体に挿入されたときに、前記 P N 信号生成のためのロジックを定めるための情報を前記 P N 発生器にあたることを特徴とする請求項 5 記載のデコーダ装置。

【請求項 7】 本体の電源の投入を検出するための電源電圧検出回路をさらに有し、前記制御部は、本体の電源の投入が検出されたときに、前記 P N 信号生成ロジックを定めるための情報を前記 P N 発生器にあたることを特徴とする請求項 1 記載のデコーダ装置。

【請求項 8】 前記制御部は、前記 P N 信号生成ロジック

クの変更を示す P N G 変更フラグが前記スクランブルされた信号とともに送られたときに前記 P N 信号生成ロジックを定めるための情報を前記 P N 発生器にあてることを特徴とする請求項 1 記載のデコーダ装置。

【請求項 9】 前記制御部は、前記 P N 信号生成ロジックを定めるための情報を複数有し、前記 P N 信号生成ロジックを定めるための情報を選択するための P N G 選択情報と前記 P N 信号生成ロジックの変更を示す前記 P N G 変更フラグとが前記スクランブルされた信号とともに送られたときに、前記 P N G 選択情報に応じた前記 P N 信号生成ロジックを定めるための情報を選択して前記 P N 発生器にあてることを特徴とする請求項 1 記載のデコーダ装置。

【請求項 10】 本体側にデコーダの I D を記憶するための I D メモリと、

前記 I D メモリに記憶された I D と前記 I C カード上の I D とが一致したときにのみ前記スクランブルキーを前記 P N 発生器にあてる比較器をさらに有することを特徴とする請求項 1 記載のデコーダ装置。

【請求項 11】 前記制御部は、前記 I D メモリに I D が記憶されていない場合に、前記 I C カード上の I D を書き込むことを特徴とする請求項 10 記載のデコーダ装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、映像及び音声信号をスクランブルして放送し、デコーダでデスクランブルして視聴する有料放送システムにおいて、受信側でデスクランブルして視聴するためのデコーダ装置に関する。

【0002】

【従来の技術】衛星を利用した放送では、映像及び音声信号をスクランブルして放送し、デコーダでデスクランブルして視聴する有料放送がある。この有料放送のシステムの一例が昭和 63 年 11 月に電気通信技術審議会により答申された「衛星放送によるテレビジョン放送における有料方式に関する技術的条件」に対する答申（文献 1）に示されている。図 9 は、文献 1 に示された有料放送のシステム構成を示したものであり、そのスクランブル方式として P N 信号（pseudo random noise：疑似ランダムノイズ信号）加算式が用いられている。

【0003】この有料放送のシステムでは、放送局 110 からデコーダ 210 に送られる放送信号には、スクランブルされた映像信号とサブ信号とが含まれ、サブ信号には、スクランブルされたデジタル音声信号及び番組情報、デコーダ 210 についての個別情報が含まれる。

【0004】放送局 110 側では、デコーダ 210 についての個別情報であるワーク鍵 Kw、契約内容、デコーダ I D のうちデコーダ I D を用いてマスタ鍵ファイル 110g からマスタ鍵 Kmi を得て、マスタ鍵 Kmi を用いて個別情報の暗号化が行われる（110f）。また、ワー

ク鍵Kwを用いて、スクランブル鍵Ks、放送局識別、サービス、年月などの番組情報の暗号化が行われる(110e)。

【0005】本件には直接関係がないためスクランブル方式の詳細は示さないが、音声信号、映像信号は、映像スクランブラ110a、音声スクランブラ110bでPN信号を使用してスクランブルされる。スクランブルのためのPN信号は、PN信号発生器110cから与えられ、その信号は順次変化するランダムデータである。PN信号発生器110cの初期状態はスクランブル鍵Ksによって与えられる。スクランブルされた音声信号は、PN信号発生器を初期化するタイミング、暗号化された番組情報及び個別情報とともに多重化されてサブ信号(副信号)となる(110d)。このサブ信号とスクランブルされた映像信号とが放送信号として放送電波として放送局110から出力される。

【0006】放送信号は、ワーク鍵Kw、マスタ鍵Kmiを用いた3重の暗号化構造によって秘話性を高めている。また、個別情報は、電話回線やICカードを介して該当するデコーダ210に送ることもできる。

【0007】デコーダ210では、放送信号のサブ信号から音声信号、番組情報、個別情報を分離する(210a)。分離された個別情報はそのデコーダのマスタ鍵Kmiを用いて復号され保存される(210f)。この復号210fは暗号化110fと同じマスタ鍵Kmiでなければ正しく行えようになっているので、当該マスタ鍵Kmiを持つデコーダのみが個別情報を復号できる。番組情報は、復号して得た個別情報のうちのワーク鍵Kwを用いて復号されるが(210e)、この場合も、暗号化110eと同じワーク鍵Kwでなければ正しく番組情報が復号できないようになっている。こうして復号して得た番組情報、個別情報は、契約条件比較回路210gで比較されて、契約条件が合いデスクランブルしても良いと判定された場合にのみ、PN発生器210cを動作させ、番組情報中のスクランブル鍵Ksを用いてPN信号を発生させる。映像デスクランブラ210a、音声デスクランブラ210bでは、このPN信号を用いて加算などによりデスクランブルが行われる。

【0008】スクランブル鍵Ksは、音声信号、映像信号をデスクランブルするのに必要な値であり、スクランブルの場合と同じ値の場合にのみ、音声信号、映像信号のデスクランブルが行われて出力される。スクランブル鍵Ksを復元するにはワーク鍵Kwを要するので、ワーク鍵Kwを持たないデコーダは正しいスクランブル鍵Ksが得られないようになっている。さらに、ワーク鍵Kwを変更可能なようにワーク鍵Kwを含む個別情報を放送局110から送出し、契約継続を望む視聴者のデコーダにのみ個別情報を与えるようになっている。そして、ワーク鍵Kwを含む個別情報を復元するにはマスタ鍵Kmiを要し、当該マスタ鍵Kmiを持つデコーダのみが個別

情報を受け取れるようになっている。マスタ鍵Kmiは、個々のデコーダごとに異なるような値に設定されている。その値は、デコーダが視聴者の手に渡る前に、例えば工場出荷時に予め設定されている。

【0009】上述のような有料放送のデコーダでは、デコーダ内の暗号復号処理や契約条件の比較といった処理はマイコンシステムを用いて行うのが一般的である。そして、このマイコンシステムを含む回路をICカードにして交換可能にすることも行われている。図10は、暗号復号処理や契約条件の比較をこのICカードで行うようにしたデコーダの構成例を示したものである。

【0010】この図10のデコーダは、図9のデコーダ210とほぼ同じ構成を有し、上記処理を行うためのマイコンシステムはICカード220に搭載されている。ICカード220とデコーダ本体とはコネクタを介して信号をやり取りできるようになっている。そして、ICカード220はマスタ鍵KmiのほかにROMなどの不揮発メモリに書き込まれたID210jを有し、デコーダ本体にはID比較器210hが設けられている。放送信号のサブ信号から分離した個別情報に含まれるIDとICカード220のID210jとをID比較器210hで比較して、一致した場合にICカード220に個別情報を与えるようにしている。番組情報、個別情報を復号し契約条件があっていた場合にスイッチ210iをONにしてスクランブル鍵KsをPN発生器210cに与えるようになっている。こうして、個別情報の選別を行い、ICカード220に与えられている個別情報からその契約者のみに視聴を制限するようになっている。なお、ID比較器210hは、ICカードとの通信データ速度に制限があるために、必要な回路である。

【0011】図11は、上記文献1に示されているPN発生器210cの構成例を示したものである。このPN発生器は、線形フィードバックシフトレジスタ(LFSR)211a、211b、211cと非線形ロジック(NF)212a、212b、212cとの組み合わせ回路例である。

【0012】スクランブル鍵Ksは、放送信号のサブ信号から得たロードタイミングパルスがあるときにLFSR211a~211cに取り込まれ、PN信号発生器の初期化が行われる。スクランブル鍵Ksのうち13ビットはLFSR211aの各レジスタに、11ビットはLFSR211bの各レジスタに、8ビットはLFSR211cの各レジスタに与えられる。

【0013】LFSR211a~211cには、音声信号、映像信号に同期したシフトクロックがあたえられており、LFSR211a~211cのレジスタのうちそれぞれ6つのレジスタからの出力がNF212a~212cに与えられる。NF212a~212cは、ROMを用いて構成され、LFSR211a~211cからの6ビット出力をそのマスクパターンに従った一定の非線

形ロジックで変換し、1ビットで出力する。切替えスイッチ214は、NF212bからの切り替え信号に応じて、NF212a、212cを切り替えて排他的論理和回路(EX-OR)213に与える。EX-OR213にはLFSR211aの1つのレジスタの出力が与えられており、これとNF212aまたはNF212cの出力のEX-ORがPN信号として映像デスクランブラ210a、音声デスクランブラ210bに出力される。

【0014】LFSR211a~211cの状態は、スクランブル鍵Ksが与えられた時の初期状態からシフトクロックに応じて遷移し、それとともなうNF212a~212cの出力も変化する。このようにランダムに変化する状態から得たランダムなPN信号をもちいてデスクランブルが行われる。

【0015】なお、この例では、NF212a~212cを用いているが、LFSR211a~211cの各1ビット分のレジスタ出力を直接切替えスイッチ214やEX-OR213に与えたり、PN信号として用いる構成もある。

【0016】

【発明が解決しようとする課題】上述のようなデコーダでは、マスタ鍵Kmi、復号アルゴリズム、PN発生器の内容が第三者に知られてしまうとシステムの安全性の低下を招くことになる。そのため、例えば図9の例では、デコーダ210に使用する映像デスクランブラ210a、音声デスクランブラ210b、PN発生器210cおよびマイコンシステムを1チップのICにするなどによって対策することが必要である。

【0017】また、図10のようにICカード220を利用したデコーダでは、ICカード220からPN発生器210cにスクランブル鍵Ksを与えることになるため、スクランブル鍵KsとPN信号の関係からPN発生器210cの構成を第三者に知られてしまう可能性があるという問題があった。

【0018】そこで、本発明はICカードを使用したデコーダでもPN発生器の安全性を向上することができるようにすることをその目的とする。

【0019】

【課題を解決するための手段】上記目的を達成するために、本願請求項1に係る発明は、スクランブルされた信号をPN信号を用いてデスクランブルするデコーダ装置であって、PN信号を用いて前記スクランブルされた信号をデスクランブルするデスクランブラと、スクランブルキーによって与えられた状態から順次状態遷移し、この遷移する状態から変換ロジックに基づいてPN信号を生成すると共に、PN信号生成のためのロジックが変更可能であるPN発生器と、スクランブルされた信号からスクランブルキーを復号すると共に、前記スクランブルキー及びPN信号生成ロジックを定めるための情報をPN発生器にあたえる制御部と、を備える。

【0020】本願請求項2に係る発明は、上記請求項1の構成に加えて、前記遷移する状態から前記PN信号を得るための信号を変換ロジックに基づいて生成すると共に、前記変換ロジックが変更可能である、非線形ロジックと、を含んで構成されていることを特徴とする。

【0021】本願請求項3に係る発明は、上記請求項1の構成に加えて、PN発生器は、スクランブルキーによって与えられた初期状態から順次状態遷移するとともに、その状態出力が変更可能であるレジスタ回路部と、レジスタ回路部の状態出力を変換しPN信号を得るための信号を生成するロジック回路部とを含んで構成されていることを特徴とする。

【0022】本願請求項4に係る発明は、上記請求項1の構成に加えて、PN発生器は、スクランブルキーによって与えられた初期状態から順次状態遷移すると共に、その状態遷移のロジックが変更可能である線形フィードバックレジスタを含んで構成されていることを特徴とする。

【0023】本願請求項5に係る発明は、上記請求項1の構成に加えて、制御部は、IDが書き込まれたICカード上に構成され、スクランブルされた信号とともに送られたIDとICカード上のIDとが一致したときにスクランブルキーをPN発生器にあたえることを特徴とする。

【0024】本願請求項6に係る発明は、上記請求項5の構成に加えて、ICカードの電源の状態を検出するための電源電圧検出回路をさらに有し、制御部は、ICカードが本体に挿入されたときに、PN信号生成ロジックを定めるための情報をPN発生器にあたえることを特徴とする。

【0025】本願請求項7に係る発明は、上記請求項1の構成に加えて、本体の電源の投入を検出するための電源電圧検出回路をさらに有し、制御部は、本体の電源の投入が検出されたときに、PN信号生成ロジックを定めるための情報をPN発生器にあたえることを特徴とする。

【0026】本願請求項8に係る発明は、上記請求項1の構成に加えて、制御部は、PN信号生成ロジックの変更を示すPNG変更フラグがスクランブルされた信号とともに送られたときにPN信号生成ロジックを定めるための情報をPN発生器にあたえることを特徴とする。

【0027】本願請求項9に係る発明は、上記請求項1の構成に加えて、制御部は、PN信号生成ロジックを定めるための情報を複数有し、PN信号生成ロジックを定めるための情報を選択するためのPNG選択情報とPN信号生成ロジックの変更を示すPNG変更フラグとがスクランブルされた信号とともに送られたときに、PNG選択情報に応じたPN信号生成ロジックを定めるための情報を選択してPN発生器にあたえることを特徴とする。

【0028】本願請求項10に係る発明は、上記請求項1の構成に加えて、本体側にデコーダのIDを記憶するためのIDメモリと、IDメモリに記憶されたIDとICカード上のIDとが一致したときにのみスクランブルキーをPN発生器にあたえる比較器をさらに有することを特徴とする。

【0029】本願請求項11に係る発明は、上記請求項10の構成に加えて、制御部は、IDメモリにIDが記憶されていない場合に、ICカード上のIDを書き込むことを特徴とする。

【0030】

【作用】本願請求項1に係る発明によれば、制御部からの情報に応じて、PN発生器のPN信号生成のためのロジックを変更することが可能であり、この変更によって生成するPN信号も異なってくる。すなわち実質的にPN発生器の構成が異なったものとして動作し、これによって得たPN信号でデスクランブルが行われるので、PN発生器のPN信号生成のためのロジック構成を解明するために、新手手間が必要になる。したがって、そのロジック構成を容易に知り得ないため、機密性を保持することができ、デコーダのセキュリティを高いものにすることができる。

【0031】本願請求項2、3又は4に係る発明によれば、PN発生器が、上記の順次状態遷移するレジスタおよび非線形ロジック又はロジック回路部で構成され、非線形ロジックの変換ロジックが変更可能であること、または、線形フィードバックレジスタの状態遷移のロジックが変更可能であることにより、PN信号生成のためのロジックを変更することが可能であり、本願請求項1と同様に、よりその内部構成を外部から分かりにくくする。

【0032】本願請求項5に係る発明によれば、IDとが一致したときにスクランブルキーがPN発生器にあたえられることにより、個別の条件に応じてデスクランブルを行う。

【0033】本願請求項6に係る発明によれば、ICカードが本体に挿入されたときに、PN信号生成ロジックを定めるための情報がPN発生器にあたえられることにより、電源オフ時にその内容が消えてしまってもよいような回路でもよいので、ハードウェアのコストが安いものにし得る。

【0034】本願請求項7に係る発明によれば、起動時にPN信号生成ロジックを定めるための情報をPN発生器にあたえるので、電源オフ時にPN信号生成ロジックを定めるための情報を保持しなくてもよい構成にし得る。

【0035】本願請求項8に係る発明によれば、PN信号生成ロジックの変更を示すPNG変更フラグがスクランブルされた信号とともに送られたときにPN信号生成ロジックを定めるための情報をPN発生器にあたえるの

で、PN発生器の動作は番組に応じて変えることができるため、番組についても機密性を保持することができ、番組のセキュリティも高いものになる。

【0036】本願請求項9に係る発明によれば、PNG選択情報とPNG変更フラグとが送られたときに、PNG選択情報に応じたPN信号生成ロジックを定めるための情報を選択してPN発生器にあたえるので、PN信号生成ロジックの選択の幅が広くなると共にPN発生器の動作は番組に応じて変えることができるため、番組についてもより機密性を保持することができ、番組のセキュリティもより高いものになる。

【0037】本願請求項10に係る発明によれば、IDメモリに記憶されたIDとICカード上のIDとが一致したときにのみスクランブルキーをPN発生器にあたえることにより、機器のセキュリティをより高めることができる。

【0038】本願請求項11に係る発明によれば、IDメモリに記憶されたIDとICカード上のIDとが一致したときにのみスクランブルキーがPN発生器にあたえられ、IDが一致したときにのみデコーダ本体の使用が可能になるので、デコーダ本体のセキュリティがより高いものになる。

【0039】

【実施例】本発明の実施例を図面を参照して説明する。なお、前述の従来例と同一もしくは同等の構成要素については同一の符号を用いると共に、その説明を簡略化しもしくは省略するものとする。

【0040】図1は、第1の実施例にかかるデコーダの構成を示したものである。このデコーダは、前述の従来例と同様に、スクランブルされた放送信号のサブ信号から音声信号、番組情報、個別情報を分離する回路210dと、放送信号のスクランブルされた映像信号をデスクランブルし映像信号にする映像デスクランブラ210a、サブ信号から得たスクランブルされた音声信号をデスクランブルし音声信号にする音声デスクランブラ210bと、個別情報に含まれるIDとICカード220のID210jとを比較するためのID比較器210hとを有する。また、このデコーダは、各種処理を行う点に付いても前述の従来例と同様であるが、マイコンシステムの一部の処理と、PN発生器310の構成が異なっており、この点に特徴がある。

【0041】PN発生器310は、スクランブルキーによって与えられた初期状態から順次状態遷移しこの遷移する状態から変換ロジックに基づいてPN信号を生成するための回路であるが、そのPN信号生成のためのロジックに変更可能部があり、すなわちPN信号生成のためのロジックが変更可能な点に特徴がある。図2および3は、このPN発生器310の構成例を示したものである。

【0042】図2のPN発生器310は、その内容が変

10

20

30

40

50

更可能な非線形ロジック (NF) 312a, 312b, 312cを用いて構成したものである。

【0043】LFSR211a~211cは、ロードタイミングパルスがあるときにスクランブル鍵Ksの13ビット、11ビット、8ビットをそれぞれ取り込み、シフトクロックに応じてLFSR211a~211cの状態は、スクランブル鍵Ksが与えられた時の初期状態から遷移する。

【0044】NF312a, 312b, 312cは、EEPROMまたはRAMなど電気的にその内容が変更可能な回路を用いて構成され、ICカード220のマイコンシステムからのPNG情報210pが書き込めるようになっている。そして、書き込まれたPNG情報210pに従った非線形ロジックで変換し、PN信号生成のための信号を1ビットで出力する。切替えスイッチ214は、NF212bからの切り替え信号に応じて、NF212a, 212cを切り替えてEX-OR213に与える。EX-OR213にはLFSR211aの1つのレジスタの出力が与えられており、これとNF212aまたはNF212cの出力のEX-ORがPN信号として映像デスクランブラ210a、音声デスクランブラ210bに出力される。

【0045】LFSR211a~211cの状態は、スクランブル鍵Ksが与えられた時の初期状態からシフトクロックに応じて遷移し、それとともなうNF212a~212cの出力も変化する。こうした状態遷移にともなうランダムなPN信号を生成する点に付いては前述の従来例と同様であるが、図2のPN発生器310では、生成されたPN信号は、NF212a~212cに書き込まれたPNG情報210pに応じて異なったものになる。

【0046】この様に、図2のPN発生器310は、非線形ロジック312a, 312b, 312cの変換ロジックを変更するようにして、PN信号生成のためのロジックを変更可能にしている。

【0047】図3のPN発生器310は、LFSR211a~211cの状態出力を可変にすることにより、等価的に変換ロジックを変更可能にしたものである。

【0048】この図3のPN発生器310は、従来例と同様のLFSR211a~211c、NF212a~212c、切替えスイッチ214、EX-OR213を用いている。そして、LFSR211a~211cとNF212a~212cとの間に、マルチプレクサ315a~315cを接続しLFSR211a~211cとともにレジスタ回路部を構成している。マルチプレクサ315aはLFSR211aの13のレジスタ出力から6つを、マルチプレクサ315bはLFSR211bの11のレジスタ出力から6つをマルチプレクサ315cはLFSR211cの8のレジスタ出力から6つをICカード220のマイコンシステムからのPNG情報210p

に基づく信号に応じて選択してNF212a~212cに与える。そして、NF212a~212cはレジスタ回路部の出力を変換してPN信号生成のための信号を得るためのロジック回路である。

【0049】こうしてLFSR211a~211cのレジスタ出力を切り替えてNF212a~212cに与えることで、PN信号生成のためのロジックが変更可能になっている。

【0050】LFSR211a~211cの一般的構成としては、図12(a)のように、M系列のPN符号を発生するものが知られている。このLFSRは、n段のシフトレジスタ2111とEX-OR2112で構成され、シフトレジスタ2111のk段(1≦k≦n)目の状態を順次EX-OR演算してシフトレジスタ2111の初段の入力として与え、シフトレジスタ2111にシフトクロックを与えることにより状態遷移していくようになっている。

【0051】LFSR211a~211cとして、本件発明者が考案した図12(b)のような回路も用い得る。この回路は、シフトレジスタ2111の所定の出力を順次EX-OR演算する第1のEX-OR2112aと、これとは異なるシフトレジスタ2111の出力を順次EX-OR演算する第2のEX-OR2112bと(さらに、第3、第4のEX-ORを設けるようにしても良い)、これらの演算結果をPNG情報210pに応じて切り替えるセレクトア2113とを有している点が、図12(b)の回路とは異なっている。この構成により、PNG情報210pに応じてLFSRの状態遷移のロジックが変更されることにより、PN信号生成のためのロジックが変更可能になっている。

【0052】図1のICカード220には、制御部であるマイコンシステムが搭載されており、図ではその処理ブロックを示している。ICカード220にはマスタ鍵Kmi及びID210jが書き込まれ、ICカード220は、従来例と同様に、分離された個別情報からマスタ鍵Kmiを用いて復号され保存する処理ブロック210f、復号して得た個別情報のうちのワーク鍵Kwを用いて番組情報を復号する処理ブロック210e、番組情報及び個別情報から契約条件を比較し契約条件が合致しているかを判断する処理ブロック210g、番組情報のうちスクランブル鍵KsをPN発生器210cに与える処理ブロック210iを有する。これらにより、従来例と同様に、マスタ鍵Kmi及びID210jが合致し、かつ、契約条件が合いデスクランブルしても良いと判定された場合に、処理ブロック210iでスクランブル鍵Ksを与えてPN発生器210cを動作させ、視聴できるようにになっている。さらに、ICカード220は、PN発生器310の変換ロジックを定めるためのPNG情報がそのROMに書き込まれ、ICカード220のマイコンシステムは、PNG情報210pをPN発生器310に与え

るようになっている。

【0053】図1のデコーダの動作は、PN発生器310およびPNG情報210pに関係するところを除いて従来例と同じである。回路210dでサブ信号から音声信号、番組情報、個別情報が分離され、個別情報に含まれるIDとICカード220のID210jとがID比較器210hで比較され、一致した場合に、ICカード220の処理ブロック210fでマスタ鍵Kmiを用いて個別情報が復号される。また、処理ブロック210eで個別情報のうちのワーク鍵Kwを用いて番組情報が復号され、処理ブロック210gで契約条件が合致していると判断されたときに、番組情報に含まれるスクランブル鍵KsがPN発生器310に与えられる。

【0054】ここで、PN発生器310はそのPN信号生成のためのロジックが変更可能であることから、すでにPNG情報210pがあれば、PN発生器310は、そのPNG情報210pに基づいて初期状態から順次状態が遷移し、それに応じたPN信号を映像デスクランブラ210a、音声デスクランブラ210bに与え、デスクランブルされた映像信号、音声信号が得られる。PN発生器310は、ICカード220のPNG情報210pが新たに与えられると、新たなPNG情報210pに基づいてその状態遷移が異なったものになり、異なったPN信号を生成し、実質的にその構成が異なったものとして動作する。こうして得た新たなPN信号でデスクランブルが行われるようになる。

【0055】この様に、このデコーダでは、PN発生器310がPN信号生成のためのロジックが変更可能であることから、PN信号生成のためのロジックが一定ではなく可変になっているので、その構成を容易に知り得ない。そのため、機密性を保持することができ、このデコーダは、セキュリティが高いものになる。

【0056】次に、第2の実施例について説明する。

【0057】この第2の実施例にかかるデコーダの構成は、図4に示すように、前述の第1の実施例と同様の構成を有するのであるが、ICカード220に電源電圧を監視する電源監視回路330が設けられている点が第1の実施例と異なっている。そして、電源監視回路330が電源がオンになるのを検知したときに、ICカード220のマイコンシステムはPNG情報210pをPN発生器310に与えるようになっている。

【0058】この第2の実施例にかかるデコーダでは、ICカード220が挿入された状態でデコーダの電源をオンにすると、電源監視回路330によって電源オンが検知される。ICカード220のPNG情報210pがPN発生器310に与えられ、PN発生器310はPN信号の生成ができるようになる。ICカード220が挿入された後の動作は第1の実施例と同じであり、PN発生器310がPN信号生成のためのロジックが変更可能であることから、機密性を保持することができ、このデ

コーダは、セキュリティが高いものになる。

【0059】この実施例の場合、起動時に、ICカード220からのPNG情報210pを与えるようにしていることから、PN発生器310は、電源オフ時にPNG情報210pを保持しておく必要はなくなる。したがって、図2のようなPN発生器310を用いた場合、電源オフ時にその内容が消えてしまってもよいような回路、例えばRAMでもよいので、ハードウェアのコストが安くなるという利点がある。

【0060】次に、第3の実施例について説明する。

【0061】この第3の実施例にかかるデコーダの構成は、前述の第2の実施例と同様の図4の構成を有するのであるが、ICカード220が挿入されたときにICカード220のマイコンシステムがPNG情報210pをPN発生器310に与えるようになっている点が異なっている。電源監視回路330はICカード220内部の電源の状態を監視し、ICカード220の挿入によって電源がオンになるのを検知したときにマイコンシステムに信号を与えるようになっており、この信号によってマイコンシステムはデコーダ本体と最初の通信の際にPNG情報210pをPN発生器310に与える。

【0062】この第3の実施例にかかるデコーダでは、ICカード220の挿入によってPNG情報210pがPN発生器310に与えられ、PN発生器310はPN信号の生成ができるようになる。ICカード220が挿入された後の動作は第1の実施例と同じであり、PN発生器310がPN信号生成のためのロジックが変更可能であることから、機密性を保持することができ、このデコーダは、セキュリティが高いものになる。この実施例の場合、電源オフ時にその内容が消えない回路、例えばEEPROMを用いることを要するが、その反面PNG情報210pがPN発生器310に保持されていることから、PNG情報210pを持っているICカード220だけでなくPNG情報210pを持っていないものも用いることができる。

【0063】次に、第4の実施例について説明する。

【0064】この第4の実施例にかかるデコーダの構成は、図5に示すように、前述の第1の実施例と同様の構成を有するのであるが、番組情報に含まれるPNG変更フラグに応じてマイコンシステムがPNG情報210pをPN発生器310に与えるようになっている点が第1の実施例と異なっている。

【0065】放送局側からは、PNG変更フラグを含む番組情報を送り、デコーダ側でPNG変更フラグを検出した場合、マイコンシステムはPNG情報210pをPN発生器310に与えてPN発生器310の動作を変更する。放送局側から番組に応じてPNG変更フラグを送ることにより、PN発生器310の動作は番組に応じて変化するようになる。そのため、番組についても機密性を保持することができ、このデコーダだけでなく番組の

セキュリティが高いものになる。

【0066】次に、第5の実施例について説明する。

【0067】この第5の実施例にかかるデコーダの構成は、図6に示すように、前述の第4の実施例と同様の構成を有するのであるが、複数のPNG情報210p1、210p2を有し、番組情報に含まれるPNG変更フラグに応じてマイコンシステムがPNG情報210pをPN発生器310に与えるうに、番組情報に含まれるPNG選択情報に応じてPN発生器310に与えるPNG情報をマイコンシステムが選択するような処理ブロック210mを有する点が第1の実施例と異なっている。

【0068】放送局側からは、PNG変更フラグ及びPNG選択情報を含む番組情報を送り、デコーダ側でPNG変更フラグを検出した場合、マイコンシステムはPNG選択情報に応じたPNG情報210p1、210p2を選択してPN発生器310に与える。PN発生器310は、PNG選択情報に応じた動作に変更される。このように、放送局側から番組に応じてPNG変更フラグ及びPNG選択情報を送ることにより、PN発生器310の動作は番組に応じて変化するようになる。そのため、番組についてより機密性を保持することができ、このデコーダだけでなく番組のセキュリティがより高いものになる。

【0069】次に、第6の実施例について説明する。

【0070】この第6の実施例にかかるデコーダの構成は、図7に示すように、前述の第1の実施例と同様の構成を有するのであるが、デコーダの側にデコーダのIDを記憶しておくためのIDメモリ330と、IDメモリ330に記憶されたIDとICカード220内のID210jとを比較する比較器410hとを有する点が第1の実施例と異なっている。そして、比較器410hは、IDメモリ330に記憶されたIDとICカード220内のID210jとが一致したときに、ICカード220からのPNG情報210をPN発生器310に与えるようになっている。

【0071】図8は、このデコーダのPNG変更の処理フローを示したもので、本実施例では、ICカード220のマイコンシステムは、上記第1の実施例の処理に加えて、IDメモリ340に関する処理を行う。

【0072】ICカード220のマイコンシステムは、IDメモリ340からよみだしてIDメモリ340にIDが記憶されているかを判定し、IDが記憶されていない場合（例えば、すべてのビットが0の場合）、ICカード220のID201jの値をIDメモリ340に書き込む、という処理を行う（図8の符号810、820）。これによって、IDメモリ340にIDが記憶されていない初期状態において場合、最初に差し込まれたICカード220のIDがデコーダ本体のIDメモリ340に書き込まれる。

【0073】電源オン後、最初に差し込まれたICカード

220のIDがIDメモリ340に記憶され、以降このIDとICカード220のIDとが比較器410hによって比較される。そして、これらが一致したときのみ、ICカード220からのPNG情報210によりPN発生器310の動作を変更できるようになる。そして、前述の実施例に示したPNG変更情報の要求があると、PNG情報210がPN発生器310に与えられる。

【0074】なお、この実施例の場合でも、ICカード220にPNG情報が無い場合は、PN発生器310の動作を変更でき無い。

【0075】この様に、この実施例では、IDメモリ340に記憶されたIDとICカード220内のID210jとを比較することによって、一致するICカード220の場合だけ、PN発生器310の動作を変更できるようになるので、機器のセキュリティをより高めることができる。

【0076】本発明は、上述の実施例に限られず、様々な変形が可能である。

【0077】例えば、第2の実施例でICカード220側に電源監視回路330が設けられているが、本体側に設けるようにしてもよい。

【0078】また、PNG情報210pはICカード220側に書き込まれたものを用いたが、PNG変更フラグとともに番組情報の中に入れて放送局側から送り、デコーダ側でICカード220のマイコンシステムが、番組情報に含まれたPNG情報210をPN発生器310に書き込むようにしてもよい。

【0079】さらに、PN発生器310は、PN信号生成のためのロジックが変更可能であればよいので、図1および2の構成に限られない。例えば、LFSRの段数を等価的にかえるように構成であってもよく、この場合、電気的にプログラム可能なロジック、例えば、フィールドプログラマブルゲートアレイ（FPGA）などを用いて構成することができる。この場合でもICカード220のマイコンシステムがPNG情報210をPN発生器310に書き込むことによってPN発生器310の動作を変更することができる。

【0080】また、図3において、ロジック回路部はNF212a～212cを用いているが通常のロジックICを用いて一定のロジックを構成するようにしてもよい。

【0081】

【発明の効果】以上の通り、本願請求項1に係る発明によれば、その構成を容易に知り得ないため、機密性を保持することができ、デコーダのセキュリティを高いものにすることができる。

【0082】本願請求項2、3又は4に係る発明によれば、PN発生器が、上記の順次状態遷移するレジスタおよび非線形ロジック又はロジック回路部で構成されるこ

とにより、よりその内部構成を外部から分かりにくくできる。

【0083】本願請求項5に係る発明によれば、IDとが一致したときにスクランブルキーがPN発生器にあたえられることにより、個別の条件に応じてデスクランブルを行いうる。

【0084】本願請求項6に係る発明によれば、ICカードが本体に挿入されたときに、PN信号生成ロジックを定めるための情報がPN発生器にあたえられることにより、電源オフ時にその内容が消えてしまってもよいような回路でもよいので、ハードウェアのコストが安いものにし得る。

【0085】本願請求項7に係る発明によれば、起動時にPN信号生成ロジックを定めるための情報をPN発生器にあたえるので、電源オフ時にPN信号生成ロジックを定めるための情報を保持しなくてもよい構成にし得る。

【0086】本願請求項8に係る発明によれば、PN信号生成ロジックの変更を示すPNG変更フラグがスクランブルされた信号とともに送られたときにPN信号生成ロジックを定めるための情報をPN発生器にあたえるので、PN発生器の動作は番組に応じて変えることができるため、番組についても機密性を保持することができ、番組のセキュリティも高いものになる。

【0087】本願請求項9に係る発明によれば、PNG選択情報とPNG変更フラグとが送られたときに、PNG選択情報に応じたPN信号生成ロジックを定めるための情報を選択してPN発生器にあたえるので、PN信号生成ロジックの選択の幅が広がると共にPN発生器の動作は番組に応じて変えることができるため、番組についてもより機密性を保持することができ、番組のセキュリティもより高いものになる。

【0088】本願請求項10に係る発明によれば、IDメモリに記憶されたIDとICカード上のIDとが一致したときにのみスクランブルキーをPN発生器にあたえることにより、機器のセキュリティをより高めることができる。

【0089】本願請求項11に係る発明によれば、IDメモリに記憶されたIDとICカード上のIDとが一致したときにのみスクランブルキーがPN発生器にあたえられ、IDが一致したときにのみデコーダ本体の使用が可能になるので、デコーダ本体のセキュリティがより高いものになる。

【図面の簡単な説明】

【図1】第1の実施例にかかるデコーダの構成を示した図。

【図2】PN信号生成のためのロジックが変更可能なPN発生器の構成例を示した図。

【図3】PN信号生成のためのロジックが変更可能なPN発生器の構成例を示した図。

【図4】第2の実施例にかかるデコーダの構成を示した図。

【図5】第3の実施例にかかるデコーダの構成を示した図。

【図6】第4の実施例にかかるデコーダの構成を示した図。

【図7】第5の実施例にかかるデコーダの構成を示した図。

【図8】第6の実施例にかかるデコーダの構成を示した図。

【図9】スクランブル放送システムの構成図。

【図10】従来例にかかるデコーダの構成を示した図。

【図11】従来例にかかるPN発生器の構成例を示した図。

【図12】LFSRの構成例を示した図。

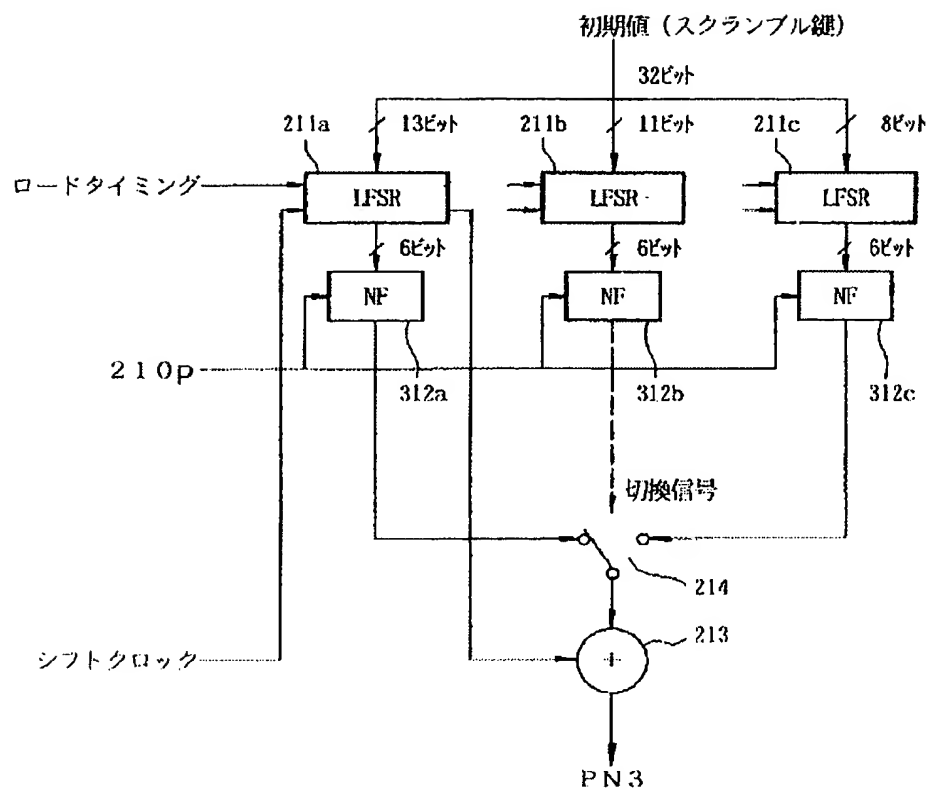
【符号の説明】

210a…映像デスクランブラ、210b…音声デスクランブラ、210j…ID、210p、210pi、210p2…PNG情報、211a～211c…LFSR、220…ICカード、310…PN発生器、312a～312c…NF、315a～315c…マルチプレクサ、330…電源監視回路、340…IDメモリ、410h…ID比較器。

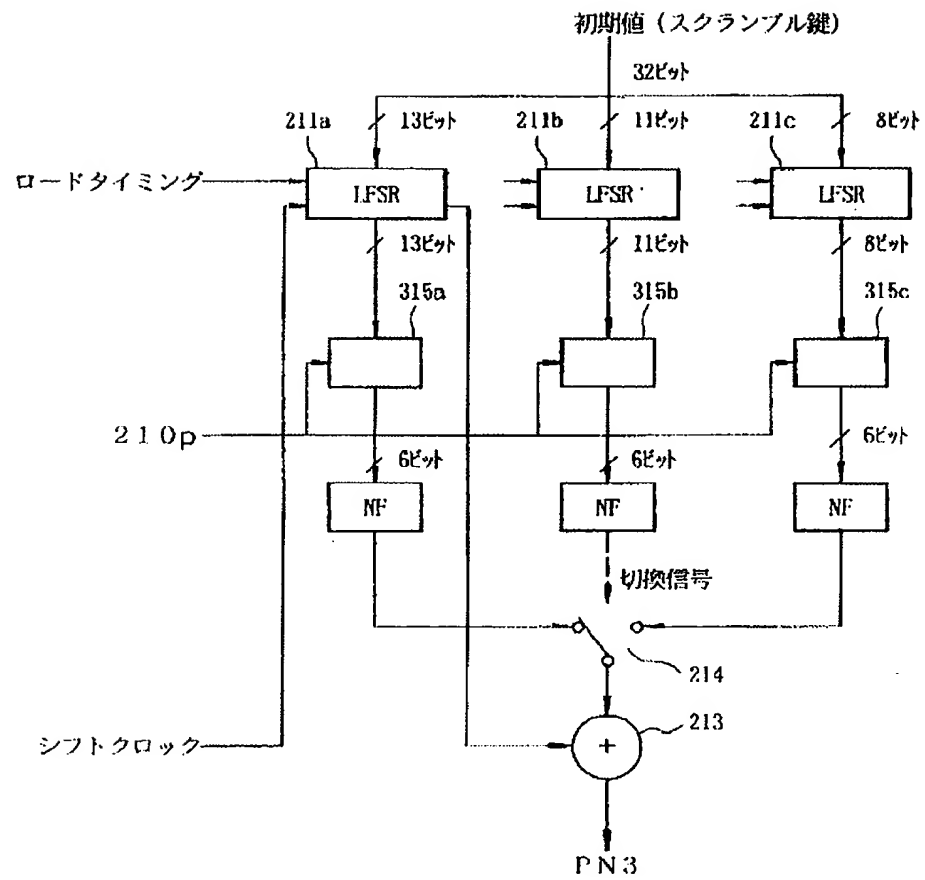
The diagram illustrates the system architecture for video recording and playback. It includes the following components and connections:

- Input:** スクラブル放送信号 (Scrambled Broadcast Signal) enters the system.
- Processing:**
 - The signal passes through a **分離** (Separation) block (210h).
 - The output of the separation block goes to an **ID比較** (ID Comparison) block (210i).
 - The ID comparison block outputs **番組情報** (Program Information) and **個別情報** (Individual Information).
 - The individual information is used by the **PN発生器** (PN Generator) (210j) and the **変更可能部** (Changeable Part) (210k).
 - The PN generator outputs **Ks** to the **映像デスクランブラ** (Video Descrambler) (210a) and the **音声デスクランブラ** (Audio Descrambler) (210b).
 - The video descrambler outputs the **映像信号** (Video Signal).
 - The audio descrambler outputs the **音声信号** (Audio Signal).
- IC Card (220):**
 - The **ICカード** (220) contains a **マスタ鍵** (Master Key) (210l) and an **ID** (210m).
 - The master key is used by the **ID比較** block.
 - The ID is used by the **ID比較** block and the **PN発生器**.
 - The IC card also contains a **復号** (Decoding) block (210n) and a **契約条件比較** (Contract Condition Comparison) block (210o).
 - The **復号** block receives **Kw** from the **ID比較** block and outputs **Kmi** to the **PN発生器**.
 - The **契約条件比較** block receives **Kmi** and outputs **変更可能部** (Changeable Part) information to the **PN発生器**.
 - The **PN発生器** also receives **変更可能部** information from the **変更可能部** block.

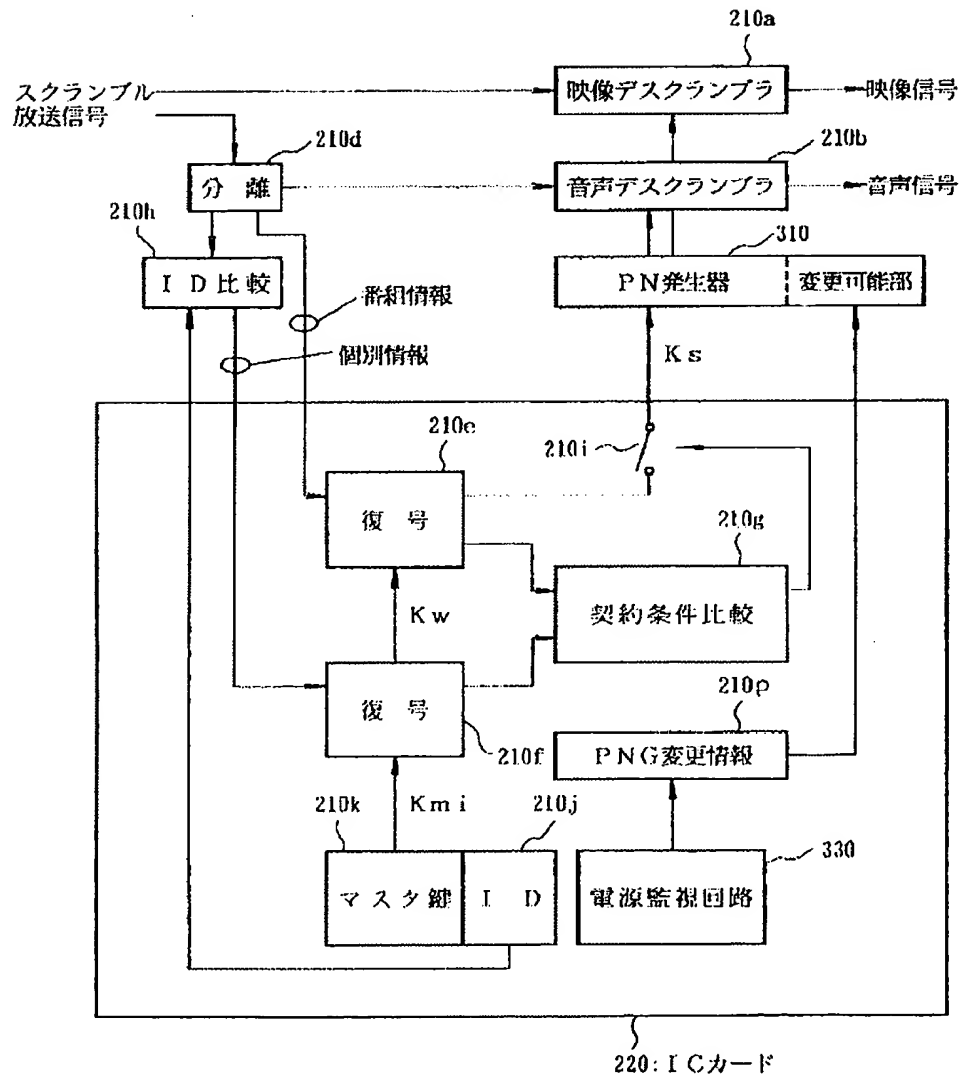
【図2】



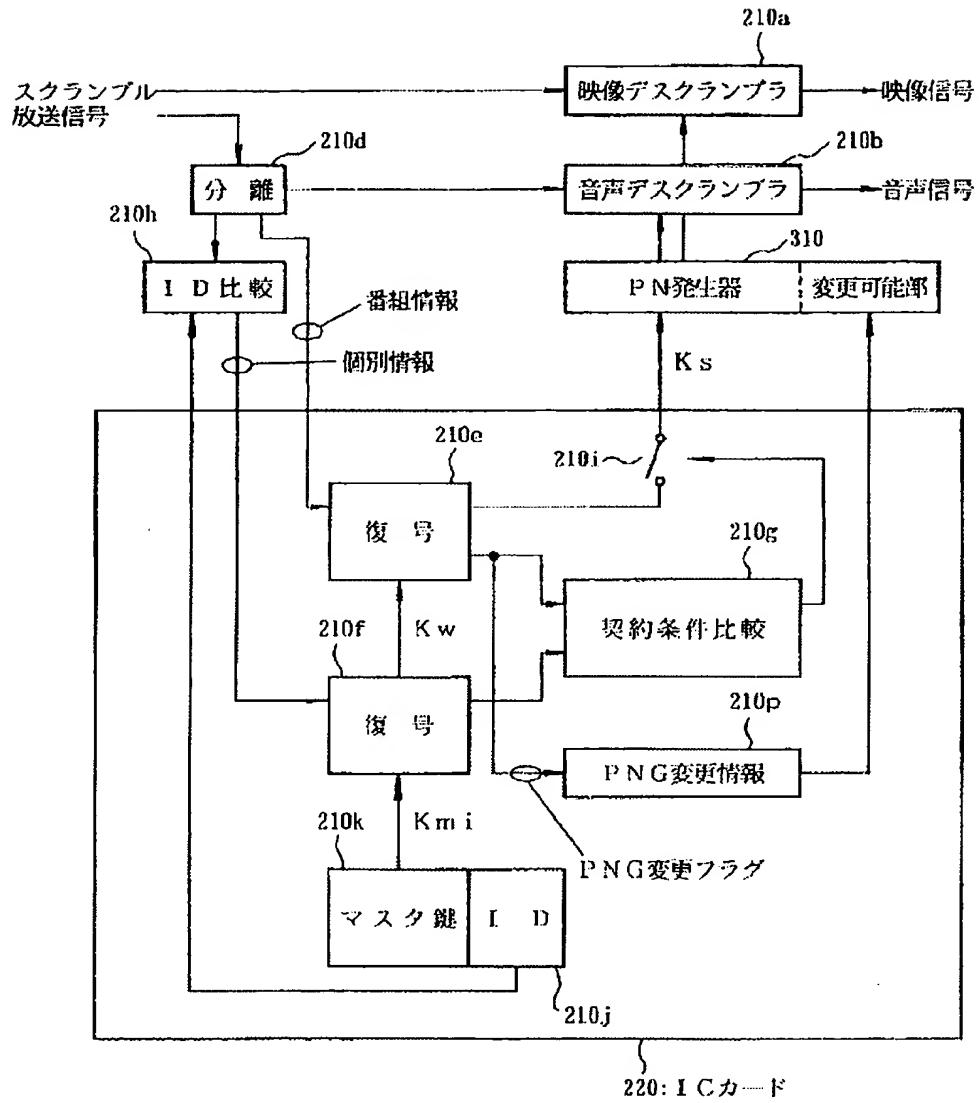
【図3】



【図4】

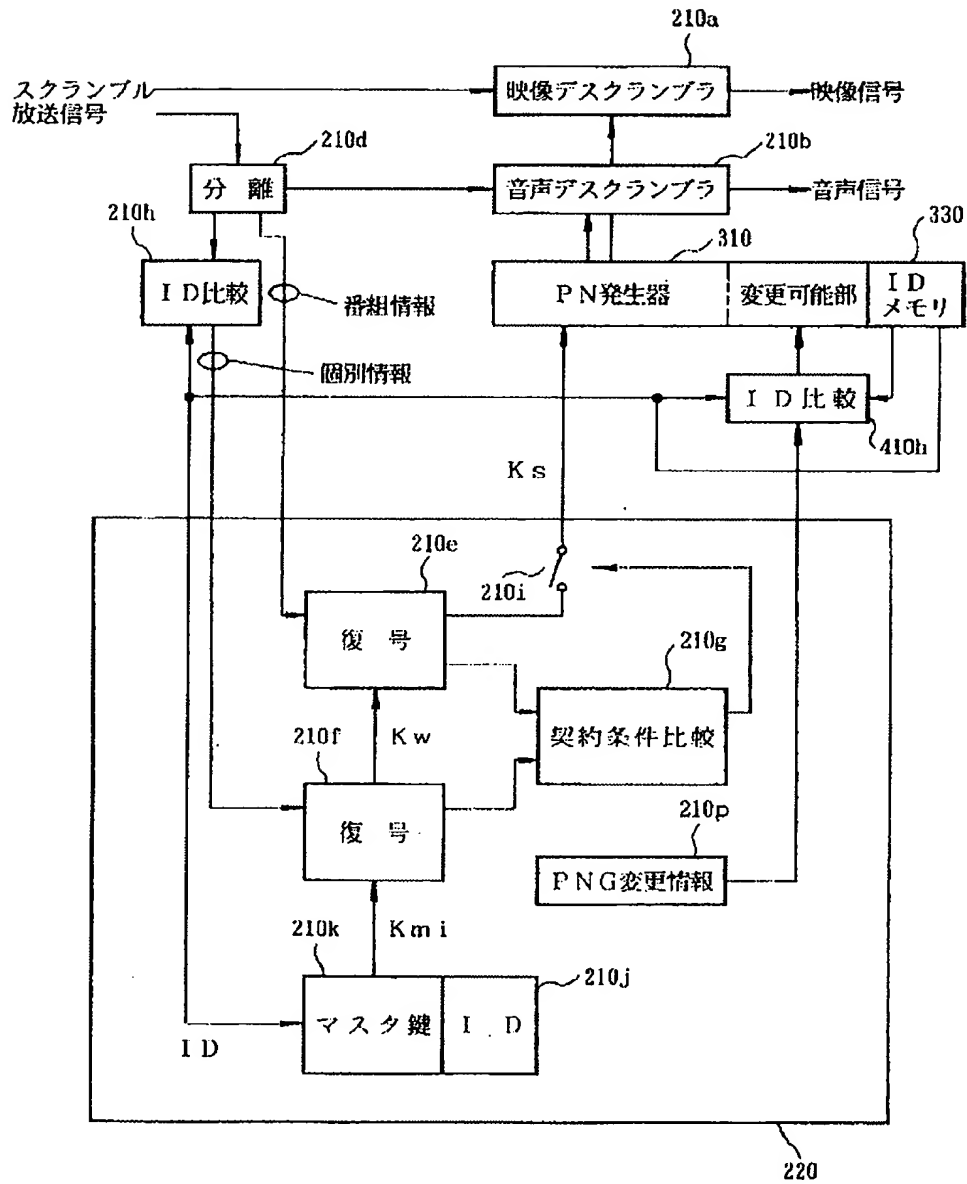


【図5】

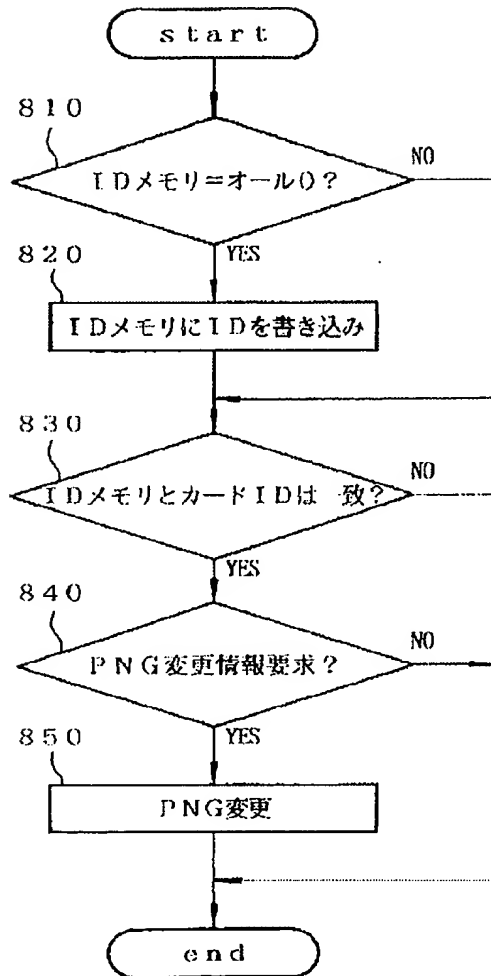


[illegible]

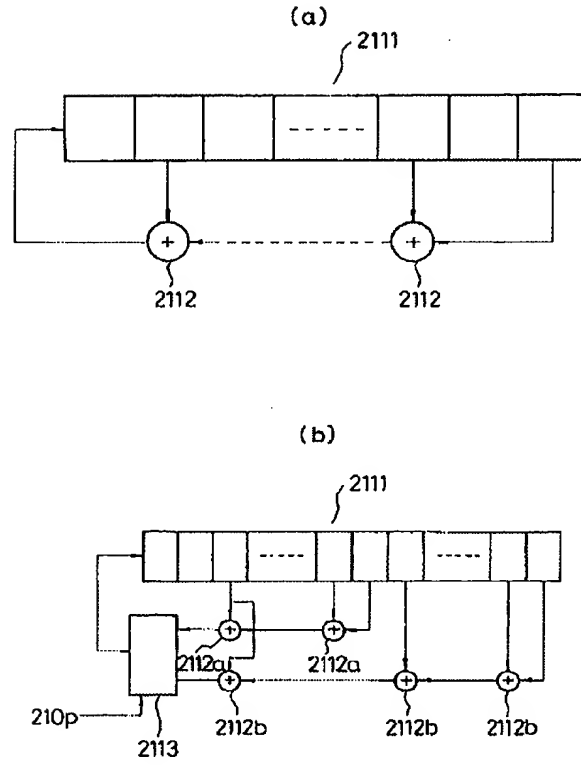
【図7】



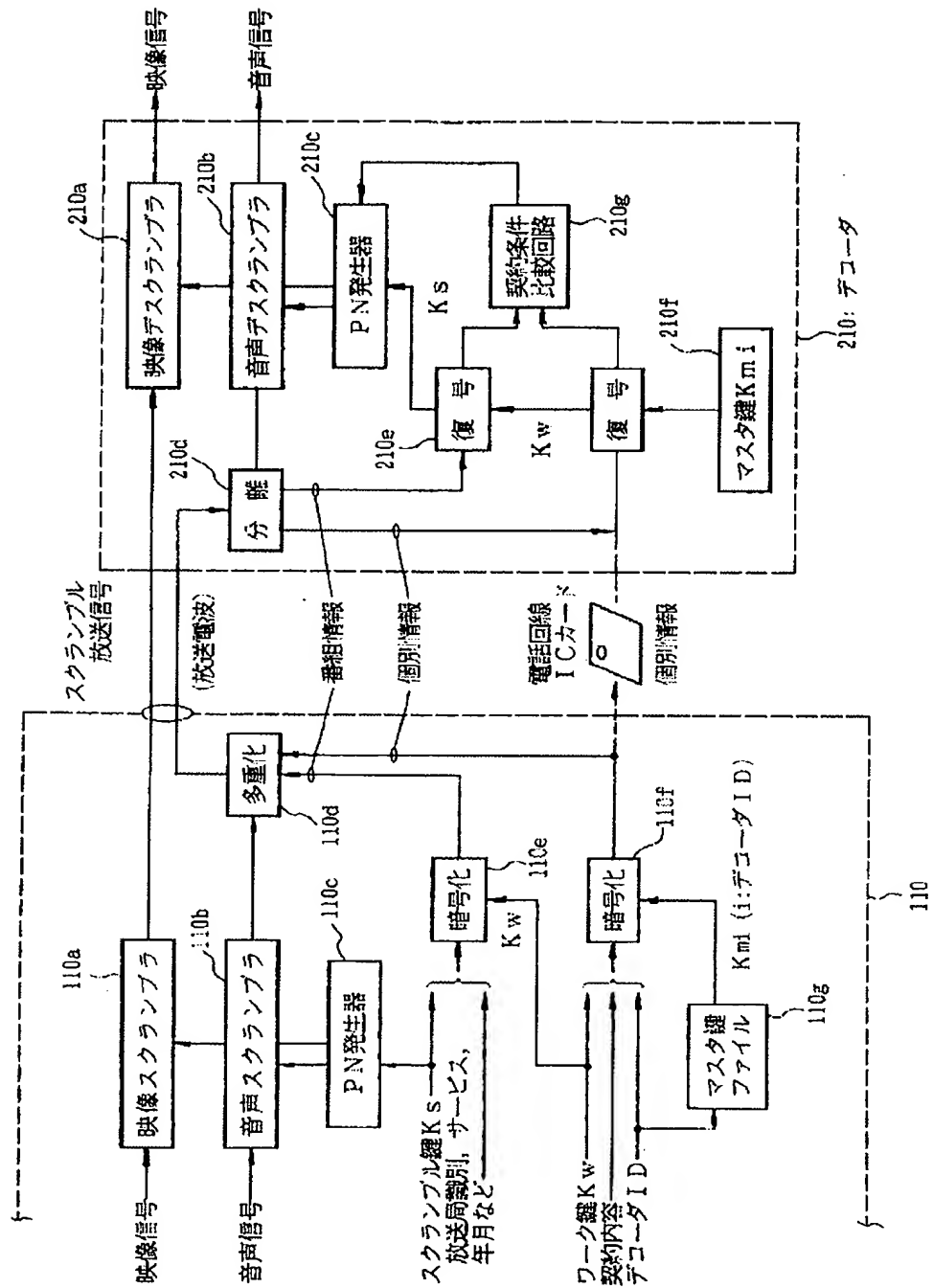
【図8】



【図12】

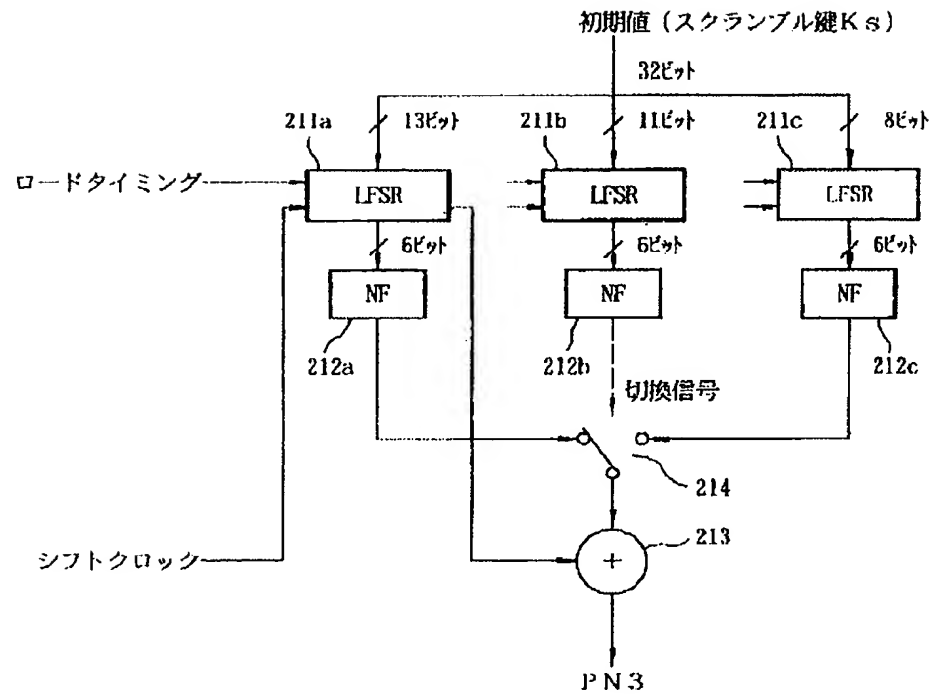


【図9】



[illegible]

【図 11】



フロントページの続き

(51) Int. Cl. 6

H04L 9/28

識別記号

庁内整理番号

F I

技術表示箇所